OLLSCOIL NA hÉIREANN, GAILLIMH

NATIONAL UNIVERSITY OF IRELAND, GALWAY

SUMMER EXAMINATIONS 2008 – HONOURS

B.A. and B.Sc EXAMINATIONS
HIGHER DIPLOMA IN MATHEMATICS

MATHEMATICS

MA416 [RING THEORY] and MA491 [FIELD THEORY]

Professor D. Armitage
Professor J. Hinde
Professor T. Hurley
Dr R. Quinlan
Dr J. Ward

Those seeking credit for one semester should answer *three* questions.
Those seeking credit for both semesters should answer *five* questions.
Please use separate answer books for each section.

Time Allowed : **Three** hours

Section A – Ring Theory (MA416)

A1. (a) Give an example of

i. A ring;
ii. A non-commutative ring;
iii. A non-commutative ring having a finite number of elements;
iv. A non-commutative ring having an uncountable number of elements;
v. A non-commutative ring that does not have an identity element for multiplication.

(b) Explain why each of the following is *not* a ring.

i. The set of non-negative integers, with the usual addition and multiplication.
ii. The set of 2×2 matrices, with real entries, whose determinant is zero (with the usual addition and multiplication of 2×2 matrices).
iii. The set of vectors in $\mathbb{R}^2$, with addition given by the usual vector addition and with multiplication given by the scalar product in $\mathbb{R}^2$.

(c) Let R be a commutative ring with an identity element for multiplication. What is meant by a *zero-divisor* in R?
What are the zero-divisors in the ring of diagonal 3×3 matrices with entries in the field $\mathbb{Q}$ of rational numbers?

(d) Let R be a commutative ring with an identity element for multiplication. What is meant by a *unit* in R? If r and s are units in R, show that their product rs is also a unit in R.

A2. (a) Let F be a field. What is meant by an *irreducible* polynomial in the ring $F[x]$ of polynomials with coefficients in F?
State the division algorithm for polynomials in $F[x]$.
Hence or otherwise show that if a polynomial $f(x)$ of degree at least 2 in $F[x]$ has a root in F, then $f(x)$ is reducible in $F[x]$.
Give an example of a polynomial in $\mathbb{Q}[x]$ that is not irreducible in $\mathbb{Q}[x]$ but has no root in $\mathbb{Q}$.

(b) Answer *true* or *false* to each of the following statements. Give a line or two of explanation for your answer in each case.

i. If a polynomial in $\mathbb{Q}[x]$ has no root in $\mathbb{Q}$, then it is irreducible in $\mathbb{Q}[x]$.
ii. If a polynomial with integer coefficients is irreducible in $\mathbb{Z}[x]$, then it is also irreducible in $\mathbb{Q}[x]$.
iii. For every positive integer n, $\mathbb{Q}[x]$ contains irreducible polynomials of degree n.
iv. If $f(x)$ is a polynomial of odd degree in $\mathbb{Q}[x]$, then $f(x)$ is reducible in $\mathbb{Q}[x]$.

(c) What is meant by a *primitive* polynomial in $\mathbb{Z}[x]$? Show that the product of two primitive polynomials is again primitive.

(d) Determine, with explanation, whether each of the following polynomials is irreducible in the indicated ring.

i. $5x^4 - 15x^3 + 12x^2 - 15x + 6$, in $\mathbb{Q}[x]$
ii. $x^4 - 4x^3 + 6x^2 - 5x - 12$, in $\mathbb{Z}[x]$
iii. $3x^3 + 2x^2 + 1$, in $\mathbb{F}_5[x]$ (here $\mathbb{F}_5$ denotes the field $\mathbb{Z}/5\mathbb{Z}$ of integers modulo 5).
iv. $2x^2 + 5x + 5$, in $\mathbb{R}[x]$.

A3. (a) Let R and S be rings.What is meant by a *ring homomorphism* $\phi : R \longrightarrow S$?
Define a function $f : M_2(\mathbb{Q}) \longrightarrow \mathbb{Q}$ by $f(A) = \det(A)$, for $A \in M_2(\mathbb{Q})$. Is f a ring homomorphism? Explain your answer.

(b) What is meant by a (two-sided) *ideal* of a ring R?
If $\phi : R \longrightarrow S$ is a ring homomorphism, define the *kernel* of ϕ and prove that it is a two-sided ideal of R.
Must the *image* of ϕ be an ideal of S?

(c) What is meant by a *principal ideal* in a commutative ring with identity?
What is meant by a *principal ideal domain (PID)*?
If F is a field, prove that the polynomial ring $F[x]$ is a PID.
Give an example, with explanation, of an integral domain that is *not* a PID.

A4. (a) What is meant by a *maximal ideal* in a commutative ring with identity?
What is meant by a *prime ideal* in a commutative ring with identity?
Give an example (with explanation) of

i. A prime ideal of $\mathbb{Z}$.
ii. An ideal of $\mathbb{Z}$ that is not prime.
iii. An ideal that is prime but not maximal, in some commutative ring with identity.

(b) Let R be a commutative ring with an identity element for multiplication. What does it mean to say that the *ascending chain condition* holds in R?
Let $C(\mathbb{R})$ denote the ring of continuous functions from $\mathbb{R}$ to $\mathbb{R}$, with addition $(+)$ and multiplication $(\times)$ defined by

$$(f+g)(x) = f(x) + g(x), \quad (f \times g)(x) = f(x)g(x), \quad \text{for } f, g \in C(\mathbb{R}),\ x \in \mathbb{R}.$$

Show that the ascending chain condition does not hold in $C(\mathbb{R})$.

(c) Give an example, with explanation, of an integral domain that is not a unique factorization domain.

Section B – Field Theory (MA 491)

B1. (a) Explain how a field $\mathbb{K}$ may be viewed as a vector space over a sub–field $\mathbb{F}$ and hence define the **degree** $[\mathbb{K} : \mathbb{F}]$.

(b) **Prove** that if $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ are fields such that $[\mathbb{L} : \mathbb{K}]$ and $[\mathbb{K} : \mathbb{F}]$ are finite, then $[\mathbb{L} : \mathbb{F}]$ is finite.

(c) Define the term **splitting field** of a polynomial. Show that $\frac{\sqrt{3}+i}{2}$ (where $i = \sqrt{-1}$) is a root of $x^4 - x^2 + 1$. Hence or otherwise find all the roots of this polynomial, and calculate the degree of its splitting field $\mathbb{K}$ over $\mathbb{Q}$.

(d) Find the minimum polynomial of $i + \sqrt{3}$ over $\mathbb{Q}(i)$. Show that $x^4 - x^2 + 1$ is reducible over $\mathbb{Q}(i)$, but does not split over $\mathbb{Q}(i)$.

(e) Deduce that $\mathbb{K} = \mathbb{Q}(i + \sqrt{3})$ is the splitting field of $x^4 - x^2 + 1$ over $\mathbb{Q}$.

B2. (a) What is meant by a "straight–edge and compass construction"?

(b) State a necessary condition for an algebraic number α to be constructible using straight–edge and compass. Is this condition also sufficient?

(c) State Gauss' Theorem concerning the values of n for which the regular n–gon can be constructed by straight edge and compass. Deduce that the angle $18°$ **is** constructible.

(d) Using the identity $\sin 3\theta = 3\sin\theta - 4\sin^3\theta$, or otherwise, **prove** that the angle $10°$ is not constructible.

(e) Show that $\cos^{-1}\left(\dfrac{23}{27}\right)$ can be trisected using straight–edge and compass.

B3. (a) Verify that $\Phi_8(x)\,(= x^4 + 1)$ factorises (reduces) in $\mathbb{Q}(\sqrt{2})$, and hence construct a splitting field for $x^4 + 1$ over $\mathbb{Q}$. If θ denotes a root of $\Phi_8(x)$, show that the other three roots are $\theta^{-1}, -\theta, -\theta^{-1}$.

(b) Consider an automorphism of $\mathbb{Q}(\theta)$, α say, such that

$$\alpha : \theta \mapsto \theta^{-1}\,.$$

How does α act on the other three roots? If β is the automorphism defined by

$$\beta : \theta \mapsto -\theta$$

find the images under β of the other three roots. Show that $\alpha\beta = \beta\alpha$ and that the group of automorphisms $\langle \alpha, \beta \rangle$ is isomorphic with the Klein 4-group.

(c) Check that $\mathbb{Q}(\sqrt{2})$ is fixed by α. Find the fields which are fixed by the automorphism β and $\alpha\beta$ respectively, and show that $x^4 + 1$ is reducible, but does not split, over each of these intermediate fields.

B4. (a) Let $\mathbb{F}_q$ be a finite field of order q $(= p^n,\ p$ a prime, $n \geq 1)$. State the main properties of $\mathbb{F}_q$.

(b) Let $f(x)$ be a monic irreducible polynomial of degree m over $\mathbb{F}_p$. Prove that $f(x)$ divides $x^{p^n} - x \Longleftrightarrow m|n$. Hence or otherwise deduce that

$$p^n = \sum_{d|n} dN_p(d)$$

where $N_p(d)$ is the number of monic irreducible polynomials of degree d over $\mathbb{F}_p$.

(c) Using the Möbius Inversion Formula, or otherwise, prove Gauss' formula

$$N_p(d) = \frac{1}{d} \sum_{k|d} \mu\left(\frac{d}{k}\right) p^k$$

where $N_p(d)$ is the number of monic irreducible polynomials of degree d over $\mathbb{F}_p$.

(d) Calculate $N_2(1)$, $N_2(2)$, $N_2(4)$ and hence, or otherwise, factorise $x^{16} - x$ into irreducible factors over $\mathbb{F}_2$.

.